

IOS IPv4 Access Lists

Standard ACL Syntax		Actions	
<div>! Legacy syntax access-list <number> {permit deny} <source> [log]</div> <div>! Modern syntax ip access-list standard {<number> <name>} [<sequence>] {permit deny} <source> [log]</div>		permit	Allow matched packets
		deny	Deny matched packets
		remark	Record a configuration comment
		evaluate	Evaluate a reflexive ACL
Extended ACL Syntax			
<div>! Legacy syntax access-list <number> {permit deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]</div> <div>! Modern syntax ip access-list extended {<number> <name>} [<sequence>] {permit deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]</div>			
ACL Numbers		Source/Destination Definitions	
1-99	IP standard	any	Any address
1300-1999		host <address>	A single address
100-199		<network> <mask>	Any address matched by the wildcard mask
2000-2699	IP extended	IP Options	
200-299	Protocol	dscp <DSCP>	Match the specified IP DSCP
300-399	DECnet	fragments	Check non-initial fragments
400-499	XNS	option <option>	Match the specified IP option
500-599	Extended XNS	precedence {0-7}	Match the specified IP precedence
600-699	Appletalk	ttl <count>	Match the specified IP time to live (TTL)
700-799	Ethernet MAC	TCP/UDP Port Definitions	
800-899	IPX standard	eq <port>	Equal to
900-999	IPX extended	neq <port>	Not equal to
1000-1099	IPX SAP	lt <port>	Less than
1100-1199	MAC extended	gt <port>	Greater than
1200-1299	IPX summary	range <port> <port>	Matches a range of port numbers
TCP Options		Miscellaneous Options	
ack	Match ACK flag	reflect <name>	Create a reflexive ACL entry
fin	Match FIN flag	time-range <name>	Enable rule only during the given time range
psh	Match PSH flag	Applying ACLs to Restrict Traffic	
rst	Match RST flag	<div>interface FastEthernet0/0 ip access-group {<number> <name>} {in out}</div>	
syn	Match SYN flag	Troubleshooting	
urg	Match URG flag	show access-lists [<number> <name>]	
established	Match packets in an established session	show ip access-lists [<number> <name>]	
Logging Options		show ip access-lists interface <interface>	
log	Log ACL entry matches	show ip access-lists dynamic	
log-input	Log matches including ingress interface and source MAC address	show ip interface [<interface>]	
		show time-range [<name>]	